



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/656,858

09/05/2003

Sonia Reed

016222-012810US

8576

20350 7590 02/01/2010
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER

DWIVEDI, MAHESH H

ART UNIT

PAPER NUMBER

2168

MAIL DATE

DELIVERY MODE

02/01/2010

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte SONIA REED and CHRISTIAN AABYE

Appeal 2009-005449
Application 10/656,858
Technology Center 2100

Decided: February 1, 2010

Before JAY P. LUCAS, JOHN A. JEFFERY, and STEPHEN C. SIU,
Administrative Patent Judges.

SIU, *Administrative Patent Judge.*

DECISION ON APPEAL
STATEMENT OF THE CASE

This is a decision on appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 13, 18, 20, 21, 23-28, 30-33, 35-40, 42-52, and 54-61. Claims 1-12, 14-17, 19, 22, 29, 34, 41, and 53 are canceled. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

Invention

The invention relates to data access and management on a secure token such as a chip card or smart card (Spec. 1, ¶ [0002]).

Independent claim 39 is illustrative:

39. A method for facilitating data management on a secure token, comprising:

providing a directory and one or more attributes associated with the directory, wherein the one or more attributes associated with the directory are used to control access to the directory by a plurality of applications associated with a client,

providing one or more cell groups under the directory, each cell group having one or more associated attributes, wherein the one or more attributes associated with a cell group are used to control access to that cell group by the plurality of applications, and

providing one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications,

wherein the one or more attributes associated with the cell group permit a first application to access that cell group after a first access condition is satisfied;

wherein the one or more attributes associated with the cell group permit a second application to access that cell group after a second access condition is satisfied; and

wherein the first access condition is different from the second access condition, and

wherein the one or more attributes associated with the directory, cell group, or cell are associated with a passcode or a key, wherein the client is adapted to use the passcode or key to access data in the directory, cell group, or cell.

References

The Examiner relies upon the following references as evidence in support of the rejections:

Carlisle	US 5,649,118	Jul. 15, 1997
Brittenham	US 6,880,084 B1	Apr. 12, 2005
Deo	US 6,970,891 B1	Nov. 29, 2005

Rejections

Claims 13, 20, 21, 23-28, 30-33, 35, 36, 38-40, 42-52, 54, 55, and 57-61 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Deo and Carlisle.

Claims 18, 37, and 56 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Deo, Carlisle, and Brittenham.

ISSUE 1

The Examiner finds that “it is clear that Deo teaches multiple applications residing on a client” (Ans. 38).

Appellants argue that Deo “does not explicitly state that a plurality of applications can exist on a single client” (Reply Br. 3).

Issue: Did Appellants demonstrate that the Examiner erred in finding that Deo teaches multiple applications residing on a client?

ISSUE 2

The Examiner finds that it would have been obvious to an artisan to combine the teachings of Deo and Carlisle because the combination “provide[s] for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card” (Ans. 39).

Appellants argue that “[if] one were to modify Deo et al. to include a client with a plurality of applications and that uses passcodes or keys to access data on a secure token, there would be no need for Deo et al.’s file system 118 and its access control mechanism, since access to directories, cell groups, and cells would already be restricted” (App. Br. 12).

Issue: Did Appellants demonstrate that the Examiner erred in finding that it would have been obvious to an artisan to combine the teachings of Deo and Carlisle?

ISSUE 3

The Examiner concludes that “no definition or explanation of what ‘share security controls’ means is listed in [claim 58]. As a result, the claim is entirely broad” (Ans. 43).

Appellants argue that “[b]y its plain meaning, an ‘agreement to share security controls’ does not include ‘any’ agreement between two entities” (Reply Br. 5).

Issue: Did Appellants demonstrate that the Examiner erred in finding that Carlisle discloses or would have suggested an agreement to share security controls?

ISSUE 4

The Examiner holds that “no definition or explanation of what a ‘loyalty application’ means is listed in [claim 59]. As a result, the claim is entirely broad” (Ans. 45).

Appellants argue that “the Examiner’s proposed reason to modify Deo et al. with a ‘loyalty application’ does not have any rational underpinning” (App. Br. 18).

Issue: Did Appellants demonstrate that the Examiner erred in finding that Carlisle discloses or would have suggested a loyalty application?

ISSUE 5

The Examiner finds that Carlisle teaches a “second application that can access [a] cell group and additional cell groups” (Ans. 47) and a “first application [that] can access only that cell group” (*id.*).

Appellants argue that the Examiner’s finding “does not have any rational underpinning” (App. Br. 20).

Issue: Did Appellants demonstrate that the Examiner erred in finding that Carlisle discloses or would have suggested a second application that can access a shared cell group, and additional cell groups, and a first application which can only access the shared cell group?

ISSUE 6

Appellants argue that “[t]he rejection of claim 60 and other claims is based on improper hindsight” (App. Br. 21).

The Examiner finds that the rejection “takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant’s disclosure” (Ans. 48).

Issue: Did Appellants demonstrate that the Examiner’s rejection depends on improper hindsight reasoning?

FINDINGS OF FACT

The following Findings of Fact (FF) are shown by a preponderance of the evidence.

1. Deo teaches that nonresident applications can “execute external to the smart card (e.g., programs on kiosks, point-of-purchase machines, etc.)” (col. 3, ll. 34-36) or be “downloaded for a particular session” (col. 3, l. 52).
2. Deo depicts a smart card in communication with “Nonresident Application(s)” (fig. 1).
3. Deo teaches that “volatile files 122 in RAM [Random Access Memory] 106 are protected by access control mechanisms of the file system 118. For example, an access control list (ACL) can be associated with each file” (col. 3, ll. 64-67). “Access control lists

and ACL tables are known in the art and are not described in detail” (col. 4, ll. 42-44).

4. Carlisle teaches that “[m]ulti-user capability is provided by allowing Root to create a subdirectory below the root directory (or a subdirectory below root) and to assign ownership of that subdirectory to another user” (col. 5, ll. 19-22).
5. Carlisle teaches “files that primarily contain information about related files [which] are called directory files or directories” (col. 4, ll. 55-56).
6. Carlisle teaches an access control system where a user can be the “owner” of [a] file, can belong to a specified “group” recognized by the file, or can belong to “other”. Each file contains a data portion that specifies the file characteristics, such as ownership, information access capabilities relative to the three types of users, etc. The owner of the file can change all file characteristics.
(Col. 4, ll. 58-64).
7. Carlisle teaches that “[i]t is quite possible for service providers to form cooperative alliances” (col. 16, ll. 66-67). “The number of . . . possibilities is limitless” (col. 17, l. 3). As an example of a cooperative alliance, “[company] A can request [gasoline provider] O to install a request for communication with [service provider] O whenever a smart card interacts with G and found to have A as a user but not [bank] B as a user” (col. 17, ll. 14-16).

8. The Specification discloses that Appellants' invention "allow[s] multiple parties with existing business relationships to access and share chip card data according to agreed security controls" (Spec. 14, ¶ [0072]).
9. The Specification discloses that an information sharing arrangement can involve an issuer, a merchant, and a third-party sponsor involved in a joint loyalty program (Spec. 14, ¶ [0074]).

PRINCIPLES OF LAW

Claim interpretation

"In the patentability context, claims are to be given their broadest reasonable interpretations. . . . [L]imitations are not to be read into the claims from the specification." *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993) (citations omitted). A claim meaning is reasonable if one of ordinary skill in the art would understand the claim, read in light of the specification, to encompass the meaning. *See In re Am. Acad. of Sci. Tech Ctr*, 367 F.3d 1359, 1364 (Fed. Cir. 2004). Any special meaning assigned to a term "must be sufficiently clear in the specification that any departure from common usage would be so understood by a person of experience in the field of the invention." *Multiform Desiccants Inc. v. Medzam Ltd.*, 133 F.3d 1473, 1477 (Fed. Cir. 1998).

Obviousness

The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art,

(2) any differences between the claimed subject matter and the prior art, and
(3) the level of skill in the art. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966).

“The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results,” *KSR Int’l Co. v. Teleflex, Inc.*, 550 U.S. 398, 416 (2007), especially if the combination would not be “uniquely challenging or difficult for one of ordinary skill in the art,” *Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1162 (Fed. Cir. 2007) (citing *KSR*, 550 U.S. at 418).

“A reference may be said to teach away when a person of ordinary skill, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the applicant.” *In re Gurley*, 27 F.3d 551, 553 (Fed. Cir. 1994).

“Patent examination is necessarily conducted by hindsight, with complete knowledge of the applicant’s invention” *In re Oetiker*, 977 F.2d 1443, 1447 (Fed. Cir. 1992). Thus, a “factfinder should be aware . . . of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning.” *KSR*, 550 U.S. at 421.

ANALYSIS

Issue 1

Appellants contest the Examiner’s finding that Deo teaches a plurality of applications on a client (App. Br. 11). Based on Appellants’ arguments,

we will decide the appeal with respect to issue 1 on the basis of claim 13 alone. *See* 37 C.F.R. § 41.37(c)(1)(vii).

Appellants' claims only require that the client have a plurality of applications; the claims do not limit where those applications execute. Thus, the claims can include either applications that execute externally or that are downloaded to the secure token for execution.

Deo teaches that a smart card can interact with nonresident applications (FF 1). One method of interaction is for the nonresident applications to execute external to the smart card (*id.*). Another method is for the smart card to download the nonresident application for a particular session (*id.*). In both cases, the smart card interacts with a client, which either provides applications for download or executes them external to the smart card. Therefore, Deo teaches multiple applications residing on a client.

Appellants contend that Deo “does not explicitly state that a plurality of applications can exist on a single client” (Reply Br. 3). However, Deo depicts a smart card in communication with “Nonresident Application(s)” (FF 2). The optional plural in this depiction would have taught or suggested a single source (client) with multiple nonresident applications. Therefore, this figure also shows that Deo would have taught or suggested multiple applications residing on a client.

For at least these reasons, we find that Appellants have not sustained the requisite burden on appeal in providing arguments or evidence persuasive of error in the Examiner's 35 U.S.C. § 103(a) rejection of claims

13, 18, 20, 21, 23-28, 30-33, 35-40, 42-52, and 54-61 with respect to this issue.

Issue 2

Appellants submit that combining Deo and Carlisle “would be contrary to the intended purpose of Deo et al.’s smartcard subsystem” (App. Br. 11). The Examiner reasons that an artisan would have been motivated “to provide for access control at higher hierarchical levels” (Ans. 39). Based on Appellants’ arguments, we will decide the appeal with respect to issue 2 on the basis of claim 13 alone. *See* 37 C.F.R. § 41.37(c)(1)(vii).

Deo teaches that volatile files in RAM are protected by access control mechanisms of the file system (FF 3). Deo includes, as an example, associating an access control list with each file (*id.*). However, Deo does not provide details about access control lists (*id.*). Nor does Deo teach or suggest that access control lists are the only appropriate access control mechanism an artisan would use. Because Deo does not provide details about access control lists, an artisan would have looked to the prior art for additional teachings. Because Deo identifies access control lists as merely an example of access control mechanisms, an artisan’s scope of inquiry would have been broader than access control lists for individual files.

Carlisle’s access control mechanisms allow for ownership (and thus access) to be set for subdirectories, not just individual files (FF 4). An artisan would have recognized that these access control mechanisms would still protect volatile files in RAM. Such an artisan would have further

recognized that allowing access control to be set for subdirectories, instead of just files, would enhance smart card security because the Root user would not have to create an access control list for each file used by an application (*id.*). Therefore, it would have been obvious to an artisan to combine the teachings of Deo and Carlisle.

For at least these reasons, we find that Appellants have not sustained the requisite burden on appeal in providing arguments or evidence persuasive of error in the Examiner's 35 U.S.C. § 103(a) rejection of claims 13, 18, 20, 21, 23-28, 30-33, 35-40, 42-52, and 54-61 with respect to this issue.

Issue 3

Appellants argue that Carlisle fails to disclose or suggest an agreement to share security controls (App. Br. 15). The Examiner concludes that claim 58 lacks a "definition or explanation of what 'share security controls' means" (Ans. 43). Appellants counter that "[b]y its plain meaning, an 'agreement to share security controls' does not include 'any' agreement between two entities" (Reply Br. 5).

Appellants submit that the "agreed security controls" limitation has a plain meaning that the Examiner fails to take into account (*id.*). Instead of making this plain meaning clear, Appellants submit an example of an agreement—agreeing to provide gas to an employee—that is not an agreement to share security controls (*id.*). However, this only serves to

illustrate one type of agreement that falls outside the scope of the claim language.

The Specification discloses that the invention “allow[s] multiple parties with existing business relationships to access and share chip card data according to agreed security controls” (FF 8). But, this does not define agreed security controls. Because neither the claim language nor the Specification clearly limits the meaning of “agreed security controls,” we hold that this limitation should be broadly interpreted to mean any shared security mechanisms available to different applications.

Carlisle teaches shared security mechanisms in the form of a file’s information access capabilities relative to users who are in a group recognized by the file (FF 6). Carlisle also teaches that the number of cooperative alliance possibilities is limitless (FF 7). An example of a cooperative alliance is an agreement in which a gasoline provider can install a request for communication with a service provider whenever a smart card interacts with the gasoline provider and the user is a particular company (*id.*). An artisan would recognize that Carlisle’s teaching of group information access capabilities would enable the implementation of cooperative alliances by allowing applications from separate parties to share data. Appellants do not show that the limitations of claim 58 are anything more than a predictable use of Carlisle’s teachings for their intended purposes.

For at least these reasons, we find that Appellants have not sustained the requisite burden on appeal in providing arguments or evidence

persuasive of error in the Examiner's 35 U.S.C. § 103(a) rejection of claims 58-60 with respect to this issue.

Issue 4

Appellants argue that Carlisle fails to disclose or suggest a loyalty application (App. Br. 17). The Examiner concludes that claim 59 lacks a "definition or explanation of what a 'loyalty application' means" (Ans. 45).

We agree with the Examiner that claim 59 does not define or explain what a loyalty application means. The Specification discloses that an information sharing arrangement can be part of a joint loyalty program (FF 9). However, this fails to define what joint loyalty programs are. Thus, we interpret a loyalty application broadly as any application associated with a preferred provider of services or goods.

Carlisle suggests that gas provider G is a preferred provider of gas for holders of a smart card issued by service provider O (FF 7). Because gas provider G is a preferred provider of goods (gas), Carlisle describes a loyalty program. Accordingly, we find that an artisan would have found it obvious that the information sharing capabilities taught by Carlisle could be used by a loyalty application. Appellants do not show that the limitations of claim 59 are anything more than a predictable use of Carlisle's teachings for their intended purposes.

For at least these reasons, we find that Appellants have not sustained the requisite burden on appeal in providing arguments or evidence

persuasive of error in the Examiner's 35 U.S.C. § 103(a) rejection of claims 59 and 60 with respect to this issue.

Issue 5

Appellants argue that Carlisle fails to disclose or suggest a second application that can access a shared cell group, and additional cell groups, and a first application which can only access the shared cell group (App. Br. 20). The Examiner finds that Carlisle teaches a “second application that can access [a] cell group and additional cell groups” (Ans. 47) and a “first application [that] can access only that cell group” (*id.*). Appellants counter that the Examiner's finding “has no rational underpinning” (Reply Br. 6).

Carlisle teaches an access control system in which a user can be the owner of a file or belong to a specified group recognized by the file (FF 6). Directories are a type of file that groups together other files (FF 5). Carlisle also teaches that the number of cooperative alliance possibilities is limitless, giving an example in which a gasoline provider installs a request for communications with a service provider (FF 7). An artisan would recognize that a first application in Carlisle could own a directory, which could also recognize access by a group that includes a second application (FF 5, 6). The artisan would further recognize that the second application could own a directory that did not recognize the shared group (*id.*). Accordingly, Carlisle would have suggested a second application that can access a shared cell group (a directory owned by the first application, but shared), and additional cell groups (a directory owned by the second application, but not shared),

and a first application which can only access the shared cell group.

Appellants do not show that the limitations of claim 60 are anything more than a predictable use of Carlisle's teachings for their intended purposes.

For at least these reasons, we find that Appellants have not sustained the requisite burden on appeal in providing arguments or evidence persuasive of error in the Examiner's 35 U.S.C. § 103(a) rejection of claim 60 with respect to this issue.

Issue 6

Appellants argue that "[t]he rejection of claim 60 and other claims is based on improper hindsight" (App. Br. 21). The Examiner finds that the rejection only takes into account "the level of ordinary skill at the time the claimed invention was made" (Ans. 48).

As shown, the prior art teaches or would have suggested all of the claim limitations identified in Appellants' arguments. Appellants do not demonstrate that combining the prior art in the suggested manner would have been uniquely challenging or difficult for one of ordinary skill.

Therefore, we are unconvinced that the rejection of claim 60 (or the other claims) depends on improper hindsight reasoning.

For at least these reasons, we find that Appellants have not sustained the requisite burden on appeal in providing arguments or evidence persuasive of error in the Examiner's 35 U.S.C. § 103(a) rejection of claims 13, 18, 20, 21, 23-28, 30-33, 35-40, 42-52, and 54-61 with respect to this issue.

CONCLUSIONS OF LAW

Based on the findings of facts and analysis above, we conclude that Appellants have not demonstrated:

1. that the Examiner erred in finding that Deo teaches multiple applications residing on a client (Issue 1);
2. that the Examiner erred in finding that it would have been obvious to an artisan to combine the teachings of Deo and Carlisle (Issue 2).
3. that the Examiner erred in finding that Carlisle discloses or would have suggested an agreement to share security controls (Issue 3);
4. that the Examiner erred in finding that Carlisle discloses or would have suggested a loyalty application (Issue 4);
5. that the Examiner erred in finding that Carlisle discloses or would have suggested a second application that can access a shared cell group, and additional cell groups, and a first application which can only access the shared cell group (Issue 5); and
6. that the Examiner's rejection depends on improper hindsight reasoning (Issue 6).

DECISION

We affirm the Examiner's decision rejecting claims 13, 18, 20, 21, 23-28, 30-33, 35-40, 42-52, and 54-61 under 35 U.S.C. § 103(a).

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

Appeal 2009-005449
Application 10/656,858

AFFIRMED

msc

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO CA 94111-3834